REMARKS:

1)   The specification has been amended as follows.

The original specification of this application was essentially a literal translation of a corresponding foreign text. The specification has now been amended in an editorial manner to improve the application's style, idiomatic English grammar, and the like, for US purposes. For example, specific reference to particular claim numbers has been avoided in the amended specification.

Certain features of the original disclosure have also been clarified. For example, it has now been more expressly stated that the input data "format" especially refers to an input data "word length", as was clear from the overall original disclosure (for example see page 3 line 1; page 4 lines 6, 16, 17 and 26 to 32; page 5 lines 10 to 12; page 6 lines 10 to 12; page 7 line 33; page 8 lines 17 to 18 and 29; etc.).

Also, it has been expressly clarified that the "encoding" or "ciphering" refers to "encryption", and that the "encoding algorithm" is thus particularly an "encryption algorithm", as supported in the original disclosure (for example see page 2 lines 3, 11, 12, 21, 29 and 30; page 4 lines 22 to 26; etc.). This amendment merely makes clear which definition of the English words "encoding" and "coding" is intended, to particularly match the meaning of the German word "Verschluesseln" used in the German priority application that was translated to prepare the original text of this US application.

4283/WFF:hc   -14-

In view of the above-mentioned original support, the present amendments do not introduce any new matter. Entry and consideration thereof are respectfully requested.

2) The claims have been amended as follows;

The original claims were essentially a literal translation of corresponding foreign claims. The original claims have now been amended in an editorial and stylistic manner to avoid undesired style aspects of the literally translated claims, and to better conform to typical US claim style, format, terminology, etc.

Claim 1 has been amended to make expressly clear that the "encoding algorithm" is particularly an "encryption algorithm" and that the "different formats" of the input data especially refer to "different input word lengths" of the input data. As discussed above regarding the specification amendments, these clarifications are supported by the original disclosure (for example see the original text portions cited above regarding the specification amendments).

Claims 5, 6, 8 and 9 have been cancelled.

The remaining dependent claims have been amended where necessary for proper conformance with the amended independent claim.

New claims 11 to 25 have been added. The new claims have been drafted "from the ground up" as a fresh approach at covering the inventive subject matter, in a different claim style, format, and terminology in comparison to the original literally translated claims. The new claims are supported by the original

4283/WFF:hc   -15-

disclosure as shown on the following table and do not introduce any new matter.

New Claims	11	12	13	14
Original Support	Cl.1; Figs.1,3,4; pg.4 ln 6– pg.5 ln 8; pg.7 ln 3– pg.8 ln 32	Cl.3; Fig.4	Cl.2; pg.6 ln 33– pg.7 ln 2	pg.4 lns 26–32

New Claims	15	16	17	18
Original Support	Fig.1; pg.4 ln 6– pg.5 ln 8; pg.6 lns 24–28	Fig.1; pg.5 lns 4–8	Figs.2a,2b,3; pg.5 ln 9– pg.6 ln 24	Cl.1,4–10; Figs.1,3,4; pg.4 ln 6– pg.5 ln 8; pg.7 ln 3– pg.8 ln 32

New Claims	19	20	21	22
Original Support	Cl.4–6	Cl.7–10	Pg.4 ln 26–32	Fig.1; pg.4 ln 6– pg.5 ln 8; pg.6 ln 24–28

New Claims	23	24	25
Original Support	Fig.1; pg.5 ln 4–8	Figs.2a,2b,3; pg.5 ln 9–pg.6 ln 24	Figs.2a,2b,3; pg.5 ln 9–pg.6 ln 24

Entry and consideration of the claim amendments and the new claims are respectfully requested.

3)   Referring to pages 2 and 3 of the Office Action, the rejection of claims 1 to 10 as obvious over US Patent 6,825,774 (Groeger) in view of US Patent 6,522,240 (Weiss et al.) is respectfully traversed.

Present independent claim 1 is directed to a contactless data transmission system having an encryption algorithm by which input data are encrypted with reference to a secret code that

4283/WFF:hc   -16-

determines particular parameters of the encryption algorithm. The encryption algorithm can be set to different input word lengths of the input data. In this regard, the data transmission system further includes a facility for setting the encryption algorithm to the respective input word lengths of the input data.

It is thus a significant feature of the present invention that the same encryption algorithm and the same device can be used for different input word lengths of the input data. In this regard, it is simply necessary to switch the encryption algorithm among the available different input word lengths, and thereby set the encryption algorithm to the proper word length pertaining to the particular input data being encrypted. As explained in the present specification, this allows the inventive data transmission system to be used in a broad range of applications, because the system is easily adaptable to different input word lengths as might arise in different applications. Also, different input word lengths provide different levels of encryption security, as well as different levels of power consumption, encryption speed, computational load, etc. Thus, by being adaptable or switchable to different input word lengths, the present data transmission system allows the end user to strike the desired balance between the required encryption security on the one hand, and the desired power saving, encryption speed, reduced computational load, or the like, on the other hand.

In contrast to the present invention, typical conventional encryption arrangements of data transmission systems operate with only a single fixed input data word length, and are thus not

4283/WFF:hc   -17-

adaptable, switchable or settable to different input word lengths. Thus, the typical conventional encryption arrangements are not easily and flexibly adaptable to different applications, and cannot achieve a variable and selectable balance between encryption security and encryption speed or power consumption or the like.

The Groeger patent discloses a remote control device in the form of a transponder for remotely controlling an electronic entertainment device such as a radio, television, or the like. The transponder includes several push buttons connected to a code generator, which generates different code signals in response to and dependent on which particular push button is pushed. The code signal is transmitted to the electronic device that is to be controlled, and a particular function of the electronic device is triggered in response to the particular code that is received. The code generator includes an encryption algorithm by which the codes may be encrypted (col 2 lines 60 to 64).

Contrary to the present invention, Groeger does **not** disclose and would **not** have suggested that the encryption algorithm can be switched among and set to different input data word lengths. More particularly, Groeger does not disclose and would not have suggested that the data transmission system must further include a facility for setting the encryption algorithm to different input word lengths.

While the Examiner has asserted that the Groeger data transmission system has a facility for setting the encryption algorithm to different "formats" of the input data, this assertion is not applicable to the clarified subject matter of

4283/WFF:hc   —18—

the present claims, namely that the "different formats" particularly involve <u>different input word lengths</u> as explained in the present specification (see e.g. page 3 line 1; page 4 lines 6, 16, 17, 26-32; page 5 lines 10-12; page 6 lines 10-12; page 7 line 33; page 8 lines 17, 18 and 29; etc.). There is no indication by Groeger that the different codes would have had different data word lengths. While the different codes generated by the code generator will have different data <u>contents</u> to convey different control information or commands, it must reasonably be understood that the different codes all have the same data word length, because there is no indication to the contrary. Since the several codes are all generated by one and the same code generator (27), it would ordinarily be expected that the various different codes all have the same data word length.

In the disclosed system, there also would have been no purpose or benefit to making the encryption algorithm switchable among different input word lengths, so a person of ordinary skill in the art would not have been motivated toward such a modification.

The Examiner has further referred to Weiss et al. for disclosing the use of a cryptographic key code. Even with such a cryptographic key code, the Weiss et al. disclosure would not have supplemented Groeger in a way that would have made the present invention obvious. Namely, Weiss et al. do not disclose and would not have suggested providing an additional facility for switching and setting the encryption algorithm to different input word lengths. Just like Groeger, Weiss et al. provide no disclosure and no suggestion that the input data to the

4283/WFF:hc   -19-

encryption algorithm can have various different input data word lengths, and provide no disclosure and no suggestion that the encryption algorithm should therefore be switchable to different input word lengths (see col. 2 lines 10 to 58; col. 3 lines 41 to 48; col. 5 lines 37 to 52; col. 6 lines 38 to 46; etc.).

Thus, even a combined consideration of the two references would not have suggested the features of present claim 1, and claim 1 would therefore not have been obvious.

The dependent claims are patentably distinguishable over the prior art already in view of their dependence from claim 1.

For the above reasons, the Examiner is respectfully requested to withdraw the rejection of claims 1 to 10 as obvious over Groeger in view of Weiss at al.

4)   The new claims 11 to 25 are also patentable over the prior art, for example as follows.

New independent claim 11 is directed to a data transmission system including two devices, of which at least one device includes an encryption unit with an <u>encryption algorithm adapted to selectively process any one of different input data having different input data word lengths</u>, as well as a control unit adapted to control the algorithm unit so as to <u>selectively process a selected one of the different input data word lengths</u> of the input data in response to a control signal. The prior art references as discussed above would not have suggested such features.

New independent claim 18 is directed to a method of contactless encrypted data transmission including a step of

4283/WFF:hc   —20—

setting an encryption device to a particular selected input data word length among different input data word lengths that can be processed by the encryption algorithm of the encryption device. The prior art references as discussed above do not include any disclosure and would not have provided a suggestion toward such a step.

For the above reasons, independent claim 11 and its dependent claims 12 to 17, as well as independent 18 and its dependent claims 19 to 25, are patentably distinguishable over the prior art.

5) Favorable reconsideration and allowance of the application, including all present claims 1 to 4, 7 and 10 to 25, are respectfully requested.
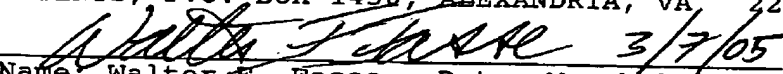
Respectfully submitted,

Dieter ANSEL
Applicant

By _____
Walter F. Fasse
Patent Attorney
Reg. No. 36132
Tel. 207-862-4671
Fax. 207-862-4681
P.O. Box 726
Hampden, ME 04444-0726

WFF:hc/4283
Enclosure:
Form PTO-2038

CERTIFICATE OF FAX TRANSMISSION:

I hereby certify that this correspondence with all indicated enclosures is being transmitted by telefax to (703) 872-9306 on the date indicated below, and is addressed to: COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA 22313-1450.

_____ 3/7/05
Name: Walter F. Fasse - Date: March 7, 2005

4283/WFF:hc

-21-